lg

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/917,368	07/27/2001	Jeffrey Scott Bardsley	RSW920010137US1	1486

26502 7590 02/22/2005

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/917,368	**Applicant(s)** BARDSLEY, JEFFREY S. ET AL.
	Examiner Jeffrey D. Popham	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 27 July 2001 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 20010727.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

Remarks

Claims 1-20 are pending.

1. Regarding Claim 3, the preamble of claim 1 states that the method is that of identifying the entry point of an attack, however, claim 3 states that the portal is an exit point, contradicting that which is in the preamble of claim 1.

Claim Objections

2. Claims 7-10 are objected to under 37 CFR 1.75(a) because of the following informalities:

- Claim 7, line 1; claim 8, line 1; and claim 9, line 2 all recite the limitation "the address". There is insufficient antecedent basis for this limitation in the claims. For purposes of prior art rejection, these claims have been viewed as being dependent upon claim 6, as opposed to claim 5.
- Claim 10, line 2: "the network data" should be "the network information".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

> applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-4 are rejected under 35 U.S.C. 102(e) as being anticipated by Yavatkar et al. (U.S. Patent 6,735,702).

Regarding Claim 1,

Yavatkar et al. disclose a method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

Obtaining intrusion information regarding an attack upon a device protected by an intrusion detection system [watchdog agent] (Column 15, lines 4-17);

Obtaining network information regarding the attack upon the device (Column 17, lines 32-51); and

Determining a portal of the attack upon the device by correlating the intrusion information and the network information (Column 18, lines 32-36).

Regarding Claim 2,

Yavatkar et al. disclose the method of claim 1, wherein the portal of the attack is an entry point of the attack (Column 18, lines 32-36).

Regarding Claim 3,

Yavatkar et al. disclose the method of claim 1, wherein the portal of the attack is an exit point of the attack (Column 14, lines 15-17).

Regarding Claim 4,

Yavatkar et al. disclose a method of identifying the entry point f an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

Obtaining intrusion information, from an intrusion detection system [watchdog agent], regarding an attack upon a device protected by the intrusion detection system (Column 15, lines 4-17);

Obtaining network information, from network equipment connected to the device regarding the attack upon the device (Column 17, lines 32-51); and

Determining a portal of the attack upon the device using a correlation engine [bloodhound agent] to correlate the intrusion information and the network information (Column 18, lines 32-36).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 5-15, 18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al. in view of Bolmarcich et al. (U.S. Patent 6,539,435).

Regarding Claim 5,

Yavatkar et al. disclose a method of identifying an entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

Obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system (Column 15, lines 4-17);

Obtaining network information, from network equipment connected to the device, regarding the attack (Column 17, lines 32-51);

Determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information (Column 18, lines 32-36);

Yavatkar et al. do not specifically disclose identifying a physical entry point associated with this logical entry point.

Bolmarcich et al., however, disclose identifying a physical entry point associated with the logical entry point (Column 1, lines 14-24). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the intrusion detection system of Yavatkar et al. with the method of using a routing table in Bolmarcich et al. in order to allow for proper routing table modifications that will prevent attack traffic from entering the network (Yavatkar et al., Column 21, lines 28-35).

Regarding Claim 6,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 5. In addition, Yavatkar et al. disclose that the intrusion information includes an address (Column 15, lines 18-21).

Regarding Claim 7,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 6. In addition, Yavatkar et al. disclose that the address is a source address (Column 15, lines 18-21).

Regarding Claim 8,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 6. In addition, Yavatkar et al. disclose that the address is a destination address (Column 15, lines 50-65).

Regarding Claim 9,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 6. In addition, Yavatkar et al. disclose that the network information includes a logical port identifier of a logical port associated with the address (Column 17, lines 38-39).

Regarding Claim 10,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 9. In addition, Yavatkar et al. disclose that the step of determining a logical entry point includes the step of finding, in the network information, the logical port identifier of the logical port associated with the address (Column 17, lines 32-51).

Regarding Claim 11,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 9. In addition, Bolmarcich et al. disclose that the step of identifying a physical entry point includes the step of identifying a physical port associated with the logical port (Column 1, lines 14-24). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the intrusion detection system of Yavatkar et al. with the method of using a routing table in Bolmarcich et al. in order to allow for proper routing table modifications that will prevent attack traffic from entering the network (Yavatkar et al., Column 21, lines 28-35).

Regarding Claim 12,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 5. In addition, Yavatkar et al. disclose that wherein the network equipment includes a network router (Column 14, lines 18-32).

Regarding Claim 13,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 12. In addition, Bolmarcich et al. disclose that the physical entry point includes a physical port of the router (Column 1, lines 14-24). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the intrusion detection system of

Yavatkar et al. with the method of using a routing table in Bolmarcich et al. in order to allow for proper routing table modifications that will prevent attack traffic from entering the network (Yavatkar et al.; Column 21, lines 28-35).

Regarding Claim 14,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 12. In addition, Yavatkar et al. disclose that wherein the logical entry point includes a logical port of the network router (Column 18, lines 32-36).

Regarding Claim 15,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 5. In addition, Yavatkar et al. disclose that the network equipment includes a firewall with routing function (Column 18, lines 54-62).

Regarding Claim 18,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 5. In addition, Yavatkar et al. disclose that the intrusion detection system includes network based intrusion detection equipment (Column 15, lines 4-17).

Regarding Claim 20,

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 5. In addition, Yavatkar et al. disclose that the intrusion detection equipment includes application based intrusion detection equipment (Column 3, lines 38-45).

5. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al. in view of Bolmarcich et al., further in view of "Network Dispatcher: a connection router for scalable Internet services", hereinafter referred to as ND.

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 5, but do not disclose that the network equipment includes a network dispatcher.

ND, however, discloses that the network equipment includes a network dispatcher (Pages 1-2, Introduction, Paragraphs 1-4). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the intrusion detection system of Yavatkar et al. as modified by Bolmarcich et al. with the network dispatcher of ND in order to spread the load of the network evenly upon multiple servers or nodes or the network.

6. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al. in view of Bolmarcich et al., further in view of Shanklin et al. (U.S. Patent 6,578,147).

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 5, but do not disclose that the network equipment includes a load balancer.

Shanklin et al., however, disclose that the network equipment includes a load balancer (Column 7, lines 39-47). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the intrusion detection system of Yavatkar et al. as modified by Bolmarcich et al. with the load balancer of Shanklin et al. in order to distribute traffic so that each intrusion detection agent processes only a portion of the traffic.

7. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al. in view of Bolmarcich et al., further in view of "Network- vs. Host-based Intrusion Detection", hereinafter referred to as NVHIDS.

Yavatkar et al. and Bolmarcich et al. disclose the method of claim 5, but do not disclose that the intrusion detection system includes host based intrusion detection equipment.

NVHIDS, however, discloses that the intrusion detection system includes host based intrusion detection equipment (Page 9, Paragraph 1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the intrusion detection system of Yavatkar et al. as modified by Bolmarcich et al. with NVHIDS in order to greatly improve network resistance to attacks and misuse, enhance enforcement of security policy, and introduce greater flexibility in deployment options.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER